14134

Monge, Elaine (SCA)

From: noreply@formstack.com
Sent: Friday, January 18, 2019 3:39 PM
To: Breaches, Data (SCA)
Subject: Security Breach Notifications

033 S. Federal Hwy #105

Formstack

Formstack Submission For: Security Breach Notifications - With Addresses

Submitted at 01/18/19 3:39 PM

Business Name:	Eltringham Law Group
Is the business located in the United States?:	Yes
Business Address:	233 Boca Raton, FL 33432
Foreign Business Address:	
Company Type:	Commercial
Your Name:	Anjali Das
Title:	Attorney
Contact Address:	55 W Monroe Street Suite 3800 Chicago, IL 60603
Contact Address:	
Telephone Number:	(312) 821-6164
Extension:	

Email Address:	Anjali.Das@wilsonelser.com
Relationship to Org:	Third party provider
Breach Type:	Electronic
Date Breach was Discovered:	12/05/2018
Number of Massachusetts Residents Affected:	3
Person responsible for data breach.:	Unknown
Please give a detailed explanation of how the data breach occurred.:	Please see letter emailed.
Please select the type of personal information that was included in the breached data.:	Social Security Numbers = Selection(s) Driver's License = Selection(s)
Please check ALL of the boxes that apply to your breach.:	The person(s) with possession of personal information had authorized access = Selection(s) The breach was a result of a malicious/criminal act. = Selection(s)
For breaches involving paper: A lock or security mechanism was used to physically protect the data.:	N/A
Physical access to systems containing personal information was restricted to authorized personnel only.:	Yes
Network configuration of breached system:	Internet Access Available
For breaches involving electronic systems, complete the following:	Personal information stored on the breached system was password-protected and/or restricted by user permissions. = Selection(s)
Does your business maintain a Written Information Security Program (WISP)?:	Yes
All Massachusetts residents affected by the breach have been notified of the breach.:	Yes

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply)::	Option2 | US Mail
Please explain your answer of Other Above:	
Date notices were first sent to Massachusetts residents (MM/DD/YYYY):	01/18/2019
All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services .:	Yes
Law enforcement has been notified of this data breach.:	Yes
Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring, including updating your WISP.:	Please see letter.
Yes / No:	Yes
File 1 Upload:	View File
File 2 Upload:	
File 3 Upload:	
File - 4 Upload:	

Formstack, 8604 Allisonville Road, Suite 300, Indianapolis, IN 46250

1341

ELTRINGHAM
LAW GROUP

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you of a data security incident at Eltringham Law Group ("ELG") that may have resulted in the disclosure of your personal information, including your name, health information, and/or Social Security number. We sincerely apologize for any inconvenience or concern this incident may cause. This letter contains information about what happened, steps you can take to protect yourself, and resources we are making available to you.

ELG learned that an unauthorized individual attempted to fraudulently wire funds from an ELG controlled account. ELG immediately launched an investigation to determine what happened. ELG retained a computer forensic firm to help identify what systems may have been accessed by unauthorized individuals and what information may have been accessible. As a result of that investigation, on December 5, 2018, we determined that some of your personal information, including your name, address, date of birth, Social Security number, driver's license number and limited health information may have been accessible by an unauthorized individual.

We have no evidence of the misuse of your information as a result of this incident, however, out of an abundance of caution and as a safeguard, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.
You have until <<Date>> to activate your identity monitoring services.
Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-???-???-????. Additional information describing your services is included with this letter.

We take the security of all information in our control very seriously and are taking steps to help prevent a similar event from occurring in the future. This includes increasing employee cybersecurity awareness training, implementing enhanced authentication controls and more robust email password policies for our employees, and adding additional security measures surrounding our internal and external communications of personal information.

Again, we sincerely apologize for any concern or inconvenience this may cause you, and we remain dedicated to protecting your information, now and in the future. Nothing is more important to us than your trust and we will continue to do whatever it takes to honor that trust because YOU are the lifeblood of our business.

If you have questions, please do not hesitate to call 1-???-???-????, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your membership number ready.

Sincerely,

David Eltringham
CEO & Founder

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:

It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General	**Rhode Island Office of the Attorney General**	**North Carolina Office of the Attorney General**	**Federal Trade Commission**
Consumer Protection Division	Consumer Protection	Consumer Protection Division	Consumer Response Center
200 St. Paul Place	150 South Main Street	9001 Mail Service Center	600 Pennsylvania Ave, NW
Baltimore, MD 21202	Providence RI 02903	Raleigh, NC 27699-9001	Washington, DC 20580
1-888-743-0023	1-401-274-4400	1-877-566-7226	1-877-IDTHEFT (438-4338)
www.oag.state.md.us	www.riag.ri.gov	www.ncdoj.com	www.ftc.gov/idtheft

For residents of Massachusetts:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf) or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.freeze.equifax.com	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monge, Elaine (SCA)

From: Potter, David H. <David.Potter@wilsonelser.com>
Sent: Friday, January 18, 2019 3:40 PM
To: Breaches, Data (SCA)
Cc: Das, Anjali C.
Subject: AG MA Notification Letter - Eltringham
Attachments: AG MA - Notification Letter - Eltringham - Submission.pdf

Please find attached a notification letter on behalf of our client, Eltringham Law Group, P.A.

Best wishes,
David

David H. Potter
Attorney at Law
Wilson Elser Moskowitz Edelman & Dicker LLP
55 West Monroe Street - Suite 3800
Chicago, IL 60603-5001
312.821.6106 (Direct)
312.704.0550 (Main)
312.704.1522 (Fax)
david.potter@wilsonelser.com

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

January 18, 2019

Anjali C. Das
312.821.6164 (direct)
Anjali.Dast@wilsonelser.com

Via Online Submission and/or Email

Attorney General Maura Healey
Office of the Attorney General
One Ashburton Place
Boston, MA 02108-1518
ago@state.ma.us

Undersecretary John C. Chapman
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116
data.breaches@state.ma.us

Re: Data Security Incident

Dear Attorney General Healey:

We represent Eltringham Law Group, P.A. ("ELG"), located in Boca Raton, FL, with respect to a potential data security incident described in more detail below. ELG takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

At the end of November, 2018, ELG learned that an unauthorized person attempted to fraudulently wire funds from an ELG controlled bank account. ELG quickly took action and notified its IT department of the incident and an investigation was undertaken. ELG retained a computer forensic company to conduct a detailed forensic investigation to determine how the unauthorized person obtained the information necessary to perpetrated the attempted fraud and what, if any, additional information may have been accessible to the unauthorized person. As a result of its investigation, on December 5, 2018, ELG discovered that two email accounts were potentially accessed by an unauthorized user and that personal information, including name, Social Security number, driver's license number and/or personal health information may have been accessible during the period of unauthorized access to the email accounts.

2. Number of Massachusetts residents affected.

A total of three (3) Massachusetts residents are known to have been potentially affected by this incident. Notification letters to these individuals were mailed on January 18, 2019, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

ELG has taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of potentially affected individuals' information. This includes, changing all passwords, increasing employee cyber security awareness training, implementing enhanced authentication controls and more robust email password policies for employees. ELG has also undertaken a review and, if necessary, an update of existing policies and procedures related to personal information. ELG has also provided potentially affected individuals with identity theft restoration and credit monitoring services for a period of twelve (12) months at no cost to the individuals, through Kroll.

4. Contact information.

ELG remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure.

ELTRINGHAM
LAW GROUP

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you of a data security incident at Eltringham Law Group ("ELG") that may have resulted in the disclosure of your personal information, including your name, health information, and/or Social Security number. We sincerely apologize for any inconvenience or concern this incident may cause. This letter contains information about what happened, steps you can take to protect yourself, and resources we are making available to you.

ELG learned that an unauthorized individual attempted to fraudulently wire funds from an ELG controlled account. ELG immediately launched an investigation to determine what happened. ELG retained a computer forensic firm to help identify what systems may have been accessed by unauthorized individuals and what information may have been accessible. As a result of that investigation, on December 5, 2018, we determined that some of your personal information, including your name, address, date of birth, Social Security number, driver's license number and limited health information may have been accessible by an unauthorized individual.

We have no evidence of the misuse of your information as a result of this incident, however, out of an abundance of caution and as a safeguard, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.
You have until <<Date>> to activate your identity monitoring services.
Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-???-???-????. Additional information describing your services is included with this letter.

We take the security of all information in our control very seriously and are taking steps to help prevent a similar event from occurring in the future. This includes increasing employee cybersecurity awareness training, implementing enhanced authentication controls and more robust email password policies for our employees, and adding additional security measures surrounding our internal and external communications of personal information.

Again, we sincerely apologize for any concern or inconvenience this may cause you, and we remain dedicated to protecting your information, now and in the future. Nothing is more important to us than your trust and we will continue to do whatever it takes to honor that trust because YOU are the lifeblood of our business.

If you have questions, please do not hesitate to call 1-???-???-????, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your membership number ready.

Sincerely,

David Eltringham
CEO & Founder

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:

It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General	**Rhode Island Office of the Attorney General**	**North Carolina Office of the Attorney General**	**Federal Trade Commission**
Consumer Protection Division	Consumer Protection	Consumer Protection Division	Consumer Response Center
200 St. Paul Place	150 South Main Street	9001 Mail Service Center	600 Pennsylvania Ave, NW
Baltimore, MD 21202	Providence RI 02903	Raleigh, NC 27699-9001	Washington, DC 20580
1-888-743-0023	1-401-274-4400	1-877-566-7226	1-877-IDTHEFT (438-4338)
www.oag.state.md.us	www.riag.ri.gov	www.ncdoj.com	www.ftc.gov/idtheft

For residents of Massachusetts:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf) or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.freeze.equifax.com	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

WILSON ELSER
WILSON ELGER MOSKOWITZ EDELMAN & DICKER LLP

January 18, 2019

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Submission and/or Email

Attorney General Maura Healey
Office of the Attorney General
One Ashburton Place
Boston, MA 02108-1518
ago@state.ma.us

Undersecretary John C. Chapman
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116
data.breaches@state.ma.us

Re: Data Security Incident

Dear Attorney General Healey:

We represent Eltringham Law Group, P.A. ("ELG"), located in Boca Raton, FL, with respect to a potential data security incident described in more detail below. ELG takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

At the end of November, 2018, ELG learned that an unauthorized person attempted to fraudulently wire funds from an ELG controlled bank account. ELG quickly took action and notified its IT department of the incident and an investigation was undertaken. ELG retained a computer forensic company to conduct a detailed forensic investigation to determine how the unauthorized person obtained the information necessary to perpetrated the attempted fraud and what, if any, additional information may have been accessible to the unauthorized person. As a result of its investigation, on December 5, 2018, ELG discovered that two email accounts were potentially accessed by an unauthorized user and that personal information, including name, Social Security number, driver's license number and/or personal health information may have been accessible during the period of unauthorized access to the email accounts.

2. Number of Massachusetts residents affected.

A total of three (3) Massachusetts residents are known to have been potentially affected by this incident. Notification letters to these individuals were mailed on January 18, 2019, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

ELG has taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of potentially affected individuals' information. This includes, changing all passwords, increasing employee cyber security awareness training, implementing enhanced authentication controls and more robust email password policies for employees. ELG has also undertaken a review and, if necessary, an update of existing policies and procedures related to personal information. ELG has also provided potentially affected individuals with identity theft restoration and credit monitoring services for a period of twelve (12) months at no cost to the individuals, through Kroll.

4. Contact information.

ELG remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure.